Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)
H1226

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on January 15, 2008

Signature /Christine Gillroy/

Typed or printed name Christine Gillroy

Application Number	Filed
10/730,621	December 8, 2003

First Named Inventor: Somnath Viswanath

Art Unit	Examiner
2136	Fikremariam Yalew

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- ☐ applicant/inventor.
- ☐ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- ☑ attorney or agent of record. Registration number 36,981
- ☐ attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____

/Thomas G. Eschweiler/
Signature

Thomas G. Eschweiler
Typed or printed name

(216) 502-0600
Telephone number

January 15, 2008
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Docket No. AMDP761US H1226

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re **PATENT** application of:

Applicant:	Somnath Viswanath
Application No.:	10/730,621
For:	METHOD AND APPARATUS FOR OUT OF ORDER WRITING OF STATUS FIELDS FOR RECEIVE IPSEC PROCESSING
Filing Date:	December 8, 2003
Examiner:	Fikremariam Yalew
Art Unit:	2136

PRE-APPEAL BRIEF IN RESPONSE TO ADVISORY ACTION DATED DECEMBER 27, 2007

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicants submit this brief in connection with the appeal of the above-identified case.

REMARKS

Claims 1-3, 5-15, and 17-21 are pending in the application. Reconsideration of the application in light of the following remarks is respectfully requested.

I. REJECTION OF CLAIMS 1-3, 5-15, AND 17-21 UNDER 35 U.S.C. § 103(a)

Claims 1-3, 5-15, abd 17-21 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Pub No. 20040128553 (Buer) in view of WO 01/05086 A2 (Krishna) and further in view of U.S. Pub No. 20020129271 A1 (Stanaway). Reversal of the rejection is respectfully requested for at least the following reasons.

i. The combination of Buer, Krishna, and Stanaway does not teach or suggest a security system comprising an output control system operable to receive at least a part of a decrypted payload of a subsequent packet before a status word of a preceding packet and the core module of the security system is operable to simultaneously decrypt and authenticate a packet payload, as recited in claims 1.

Claim 1 is directed to a network interface system for interfacing a host system with a network to provide outgoing data from the host system to the network and to provide incoming data from the network to the host system. The network interface system comprises a security system operable to receive at least a part of a decrypted payload of a subsequent patent before a status word of a preceding packet.

The Office Action concedes that Buer and Krishna do not teach or suggest an output control system operable to receive at least a part of a preceding packet before a status word of a preceding packet and a core module of the security system operable to simultaneously decrypt and authenticate a packet payload. In addition, further combining Stanaway to the teachings of Buer and Krishna does not remedy their deficiency.

As highlighted in applicants' specification, a status word is different than payload data because it resides at the end of a packet, and includes trailers received from the network and information that the network interface system inserts at the end of the packet (*see, e.g.*, page 8, line 27 - page 9 line 2). Claim 1 is not obvious by the combination of the cited references because the session discussed in Stanaway at paragraph 0019 is a user-VPN session that occurs after accessing a virtual private network wherein processing of the packets flows **in sequential order with no mention of any out-of order processing wherein a part of a decrypted payload being received before the status words of a preceding packet**. For example, Stanaway states in paragraph 0019 the following:

> If the present request for a VPN is not the first communication between security gateway and the user, the gateway controller accesses the previously negotiated SA (security association) from storage, stores it in the gateway data engine and binds it to the IP address of the user as assigned by the ISP. As subsequent packets are received in the same session the data engine accesses the Security Association (SA) bound to the assigned user IP address and properly decrypts the packet payload.

Stanaway explains that "subsequent packets" are received in the same session (i.e., the VPN session) and then decrypted. This teaches a **sequential data flow** processed in the order of packets received after a user VPN connection is established or authenticated and not an out of order processing as recited in claim 1. Then in paragraph 0020, Stanaway further explains that, ***"[a]fter*** **the user of a VPN is authenticated,** VPN packets can be properly received and decrypted for communication." This is very different from a decrypted payload of a subsequent packet being received before the status word of a preceding packet and the core module of the security system being operable to simultaneously decrypt and authenticate a packet payload, as recited in claim 1.

As explained in the specification on page 10, lines 4-16, the result of authentication is the status word. Where the data is written "in-order," the decrypted data for a first packet is followed by the status word. This type of sequential order is what Stanaway performs according to the detailed description at paragraph 0020 wherein after a VPN session is established by user name/password subsequent packets are received and then decrypted. Out-of-order writing means that decryption of the subsequent packet can begin prior to generating the status word for the current packet. Consequently, **"in-order" processing, as explained by Stanaway is not operable to receive at least a part of a decrypted payload of a subsequent packet preceding before a status word of a preceding packet and the core module of the security system being operable to simultaneously decrypt and authenticate a packet payload**, as recited in claim 1. Withdrawal of the rejection is therefore respectfully requested.

The type of authentication in Stanaway is for establishing a virtual private network (VPN) connection which is different from decrypting and authenticating data packets for communication transmission between a network and a network peripheral, as appreciated by one of ordinary skill in the art. Establishing a VPN session requires a user name and/or password ID (see, paragraph 0018), as compared to transmission of data packets from a network to a network peripheral for communication which requires decrypting and authenticating the data packets. Therefore, Stanaway would render the

cited invention inoperable for purposes of establishing a VPN session by not authenticating the session and then receiving and decrypting packets. This is very different from what is claimed in claim 1 reciting a decrypted payload of a subsequent packet being received before the status word of a preceding packet and the core module of the security system being operable to simultaneously decrypt and authenticate a packet payload.

ii. The combination of Buer, Krishna, and Stanaway does not teach or suggest a core module operable to decrypt completely the subsequent packet prior to authenticating the current packet, as recited in claim 13.

Claim 13 recites a network interface system for interfacing a host system with a network to provide outgoing data from the host system to the network and to provide incoming data from the network to the host system. The network interface system comprises a core module operable to decrypt completely the subsequent packet prior to authenticating the current packet.

The same rationale as above is reiterated by demonstrating that Stanaway explicitly teaches that *"[a]fter* **the user of a VPN is authenticated,** VPN packets can be properly received and decrypted for communication." Because subsequent packets are received and decrypted **after authentication**, Stanaway does not teach or suggest that a core module is operable to decrypt completely the subsequent packet prior to authenticating the current packet, as recited in claim 13.

Stanaway further explains that subsequent packets are not completely decrypted prior to authenticating the current packet as recited in claims 1 and 13 at paragraph 0028. Stanaway states that **"[a]fter the session is authenticated** and the memory is written, data packets are received at the data engine." This is in contrast to claims 1 and 13 and therefore withdrawal of the rejection is respectfully requested.

Accordingly, reversal of this rejection is respectfully requested for at least the above reasons.

II. CONCLUSION

For at least the above reasons, the claims currently under consideration are believed to be patentable over the cited references. Accordingly, it is respectfully requested that the rejections of the pending claims be reversed.

For any extra fees or any underpayment of fees for filing of this Brief, the Commissioner is hereby authorized to charge the Deposit Account Number 50-1733, AMDP761US.

Respectfully submitted,
ESCHWEILER & ASSOCIATES, LLC

By /Thomas G. Eschweiler/
Thomas G. Eschweiler
Reg. No. 36,981

National City Bank Building
629 Euclid Avenue, Suite 1000
Cleveland, Ohio 44114
(216) 502-0600